Romain Jacquet **BTS SIO 1**
18/12/2025

Compte rendu TP TH3 : CH4 : TD1

Sommaire

Introduction

L'objectif de ce TP est de découvrir différentes méthodes de cassage de mots de passe afin de comprendre leurs faiblesses. Pour cela, nous avons utilisé deux machines virtuelles : Windows 10 et Kali Linux. À l'aide des outils John the Ripper et Ophcrack, nous avons testé plusieurs techniques pour retrouver des mots de passe et analyser leur efficacité.

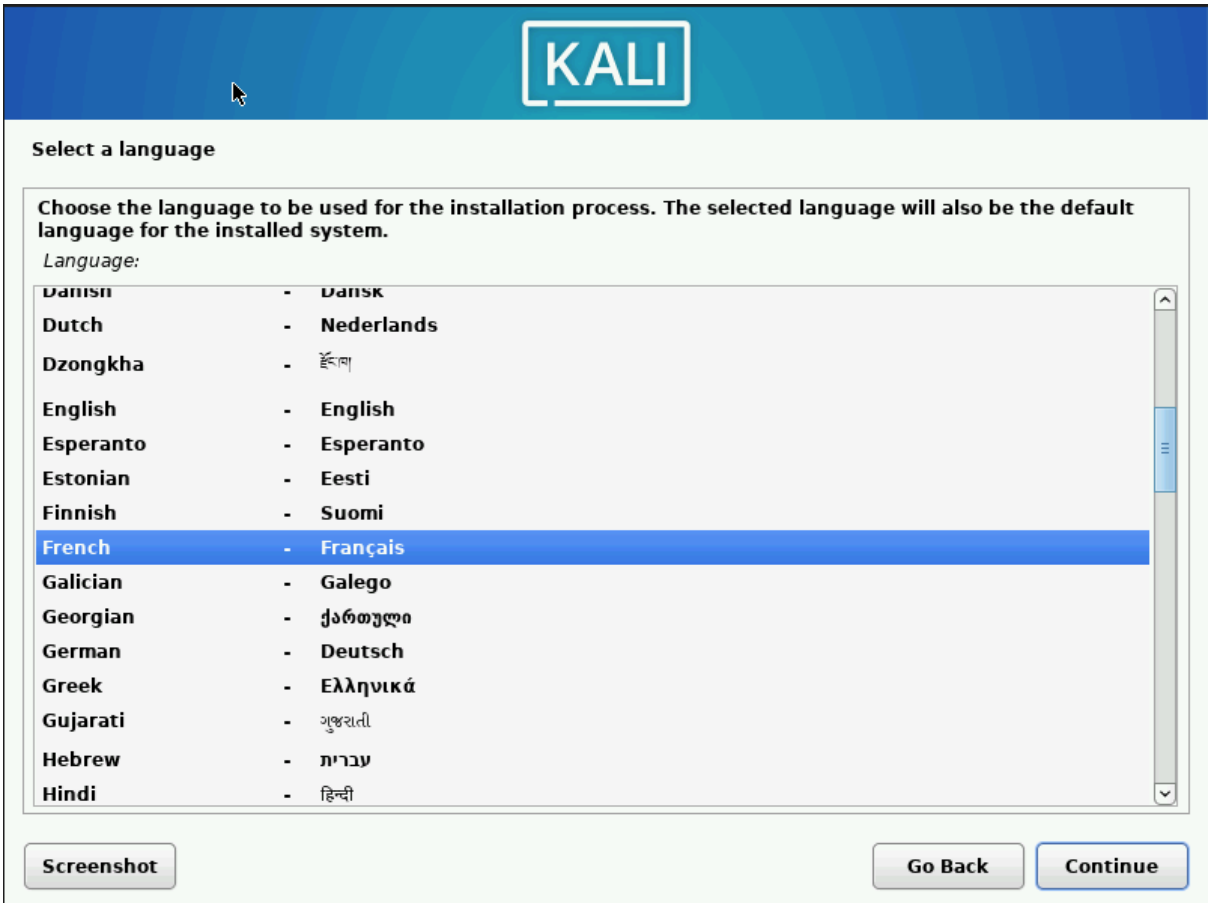
1.

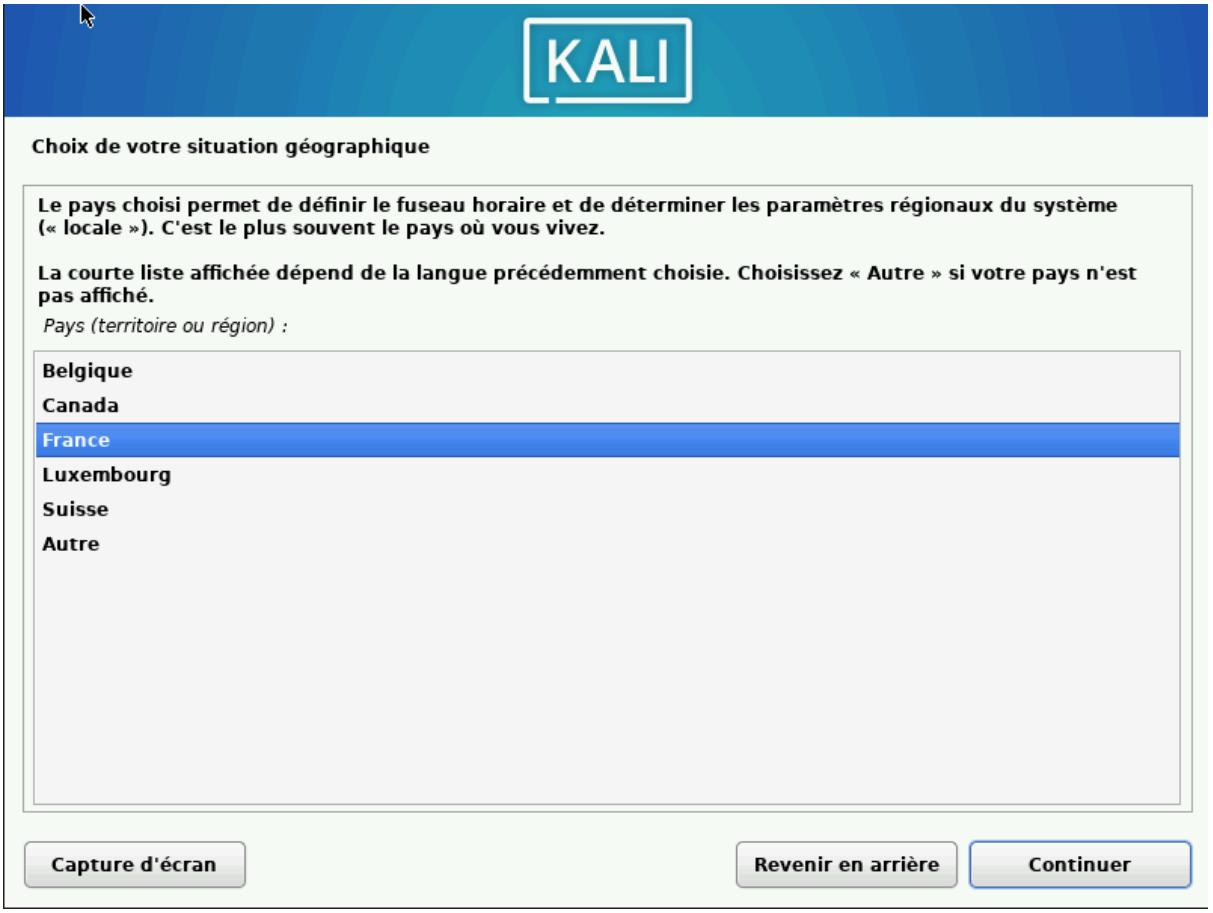
Premièrement j'ai télécharger la VM Windows 10 en suivant le lien ci dessous :
www.lienmini.fr/882-03

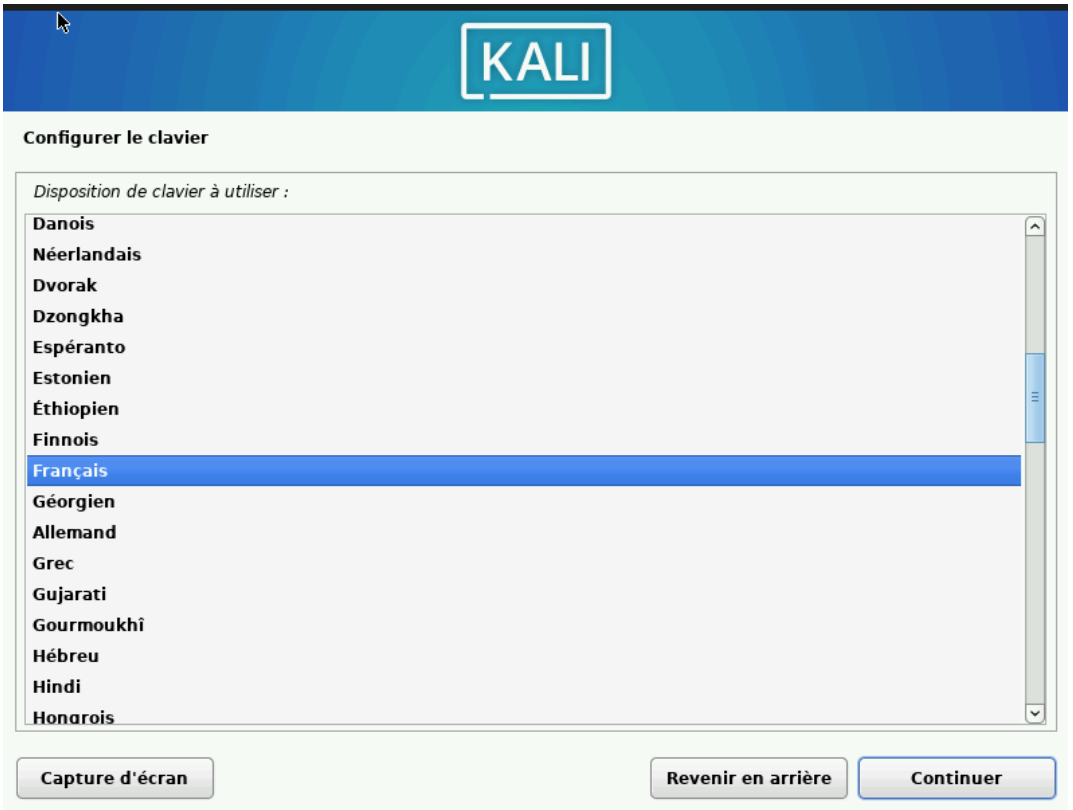
2.

Deuxièmement j'ai télécharger la VM Kali en suivant le lien :
http://www.lienmini.fr/882-04

Voici ci dessous tous les réglages :




KALI
Choix de votre situation géographique
Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.
La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.
Pays (territoire ou région) :
Belgique
Canada
France
Luxembourg
Suisse
Autre
Capture d'écran
Revenir en arrière
Continuer


KALI
Configurer le clavier
Disposition de clavier à utiliser :
Danois
Néerlandais
Dvorak
Dzongkha
Espéranto
Estonien
Éthiopien
Finnois
Français
Géorgien
Allemand
Grec
Gujarati
Gourmoukhi
Hébreu
Hindi
Hongrois
Capture d'écran
Revenir en arrière
Continuer

3.

J'ai utilisé l'outil John the Ripper en ligne de commande pour tester trois techniques différentes:

- L'attaque "Single" : J'ai lancé la commande `john -single`. L'outil essaie de deviner le mot de passe en modifiant simplement le nom d'utilisateur (ex: enedis123). C'est très efficace contre les gens qui manquent d'imagination.

- L'attaque par Dictionnaire : J'ai utilisé une liste de mots de passe connus (comme le fichier `rockyou.txt` ou `password.lst`). Si le mot de passe est un mot courant, John le trouve direct.

- La "Force Brute" : Avec la commande `john -incremental`, l'ordinateur teste toutes les combinaisons possibles. C'est la méthode la plus sûre pour trouver, mais c'est extrêmement long si le mot de passe est complexe.

4.

J’ai fait les test avec Ophcrack (Tables Arc-en-ciel)

Pour finir, j'ai testé une autre méthode avec le logiciel Ophcrack. Au lieu de calculer les combinaisons une par une, j'ai chargé une "Rainbow Table" (la table `vista_proba_free`). C'est comme une énorme base de données de solutions pré-calculées. J'ai chargé mon fichier `pwdump`, installé la table, et cliqué sur "Crack". C'était impressionnant de voir la vitesse à laquelle les mots de passe simples sont apparus.

5.

J'ai lancé le logiciel Ophcrack. J'ai chargé mon fichier de mots de passe avec le bouton Load, puis j'ai installé la table arc-en-ciel `vista_proba_free` via le bouton Tables. Enfin, j'ai cliqué sur Crack. L'outil a retrouvé les mots de passe très vite grâce à la table pré-calculée.

6.

Pour qu'un mot de passe soit sûr, j'ai compris qu'il faut respecter 3 règles :

- La Longueur : Il faut plus de 8 caractères (les courts se font pirater trop vite).
- La Complexité : Il faut mélanger des majuscules, minuscules, chiffres et symboles. Surtout pas de mots du dictionnaire.
- L'Aléatoire : Ne jamais utiliser son nom ou son identifiant dans le mot de passe.

Conclusion

Ce TP nous a permis de constater que les mots de passe simples sont faciles à casser, surtout avec des outils spécialisés. Les attaques par dictionnaire, force brute et tables arc-en-ciel montrent l’importance d’utiliser des mots de passe longs, complexes et aléatoires. En conclusion, un mot de passe bien choisi est essentiel pour assurer la sécurité d’un système.